Abstract

A single card can manage and deliver multiple applications
5   such as cash replacement, loyalty, membership, access,
healthcare, and transportation. This "sharing" of a card,
however, presents numerous challenges for keeping the application
data separate and retaining ownership. A method is described for
the secure allocation and control of card resources.
10   Specifically, application providers can be given control over
their own specific application domain, yet the card issuer still
retains ultimate ownership control of the card and therefore can
dictate what applications can be loaded.

Each application will have its own space on the card
15   firewalled from others. Further, these applications can be added
or erased dynamically even after the card is in circulation. In
particular, the structure of a standard smart card can be
organized so that different applications are secure and separate.
The permission to create and load these applications can be
20   granted exclusively by the card issuer.